UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/694,824	10/29/2003	Antonio Lain	200205659-2	7594

22879 7590 04/02/2007

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
GERGISO, TECHANE	
ART UNIT	**PAPER NUMBER**
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/694,824	LAIN ET AL.	
	Examiner	Art Unit	
	Techane J. Gergiso T-G	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 January 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *01/17/07;11/14/05;03/17/0410*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is a non-Final Office Action in response to the applicant's communication filed on January 17, 2007.

2. Claims 1-14 have been examined.

3. Claims 1-14 are pending.

Claim Objections

4. Claim 13 is objected to because of the following informalities: Claim 20: line 13: recites, "security **keys keys** generated." One "**keys**" is not needed. Appropriate correction is required.

5. Claims 8, 10, 11 and 14 are objected to because of the following informalities:

The term "**Placebo keys**" in claim 8, 10, 11, and 14 is used by the applicant in the claims to mean "inactive or temporal keys", while the accepted meaning is:" a. A substance containing no medication and prescribed or given to reinforce a patient's expectation to get well. b. An inactive substance or preparation used as a control in an experiment or test to determine the effectiveness of a medicinal drug. OR. Something of no intrinsic remedial value that is used to appease or reassure another." American Heritage Dictionary, 4th Edition. The term is indefinite because the specification does not clearly redefine the term and the claims are rendered ambiguous.

Appropriate correction is required.

Specification

6. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

[Disclosure; 0022] More complete information may however be obtained from "Key Management for Multicast: Issues and Architectures; D. Wallner, E. Hardner & R. Agee, available online at the website **www.ietf.org/rfc/rfc2627.txt** the contents of which are hereby incorporated by reference.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-9 and 13 rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech et al. (hereinafter referred to as Lotspiech, US Pat. No.: 7,039,803), in view of Sudia et al. (hereinafter referred to as Sudia, US Pub No.: 2002/0029337).

As per claim 1:

Lotspiech discloses a method of managing security keys generated from an ancestral hierarchy and used to provide selective access to provision of a service, wherein invalidation of a key necessitates reconfiguration of each other key within the hierarchy to the extent another key and an invalidated key share common ancestry, the method comprising the steps of:

defining at least two groups of users of the service to whom keys have been issued (column 3: lines 5-21; column 4: lines 37-60; column 6: lines 20-37);

issuing keys to users from domains within the hierarchy upon the basis of their grouping (column 3: lines 11-20, lines 53-64; figure 4:36, 38; Column 7: lines 55-65).

Lotspiech does not explicitly disclose allocating within the hierarchy a distinct domain for each group of users. Sudia, in analogous art, however, teaches allocating within the hierarchy a distinct domain for each group of users (0046-0050). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Lotspiech to include allocating within the hierarchy a distinct domain for each group of users. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to provide a system for securely using digital signatures in a commercial cryptographic system that allows industry-wide security policy and authorization information to be encoded into the signatures and certificates by employing attribute certificates to enforce policy and authorization requirements as suggested by Sudia in (0024).

As per claim 2:

Sudia discloses a method, wherein the at least two groups of users are defined upon the basis of a predetermined policy which provides that users are grouped according to their perceived value to a provider of the service (0024; 0053; 0055).

As per claim 3:

Lotspiech discloses method, wherein a first user group having the highest perceived value to the provider are allocated keys from a first domain, and wherein keys from the first domain share fewer ancestors with keys from other domains than said keys from other domains share with each other (Column 4: lines 37-50; column 10: lines 3-22).

As per claim 4:

Lotspiech discloses method, wherein keys from the first domain share only one ancestor with said keys from other domains (column 4: lines 40-60).

As per claim 5:

Lotspiech discloses method, wherein the ancestral hierarchy has a binary tree architecture (column 3: lines 15-22).

As per claim 6:

Sudia discloses a method, wherein the at least two groups of users are defined upon the basis of a predetermined policy which provides that users are grouped according to a perceived susceptibility of them ceasing to require the service, and a first user group having the highest

perceived susceptibility are allocated keys from a first domain, and wherein keys from the first domain share fewer ancestors with keys from other domains than said keys from other domains share with each other (0024; 0053; 0055; 0046-0050).

As per claim 7:

Lotspiech discloses method, wherein keys from the first domain share only one ancestor with said keys from other domains (column 4: lines 40-60).

As per claim 8:

Sudia discloses a method, wherein varying levels of service are available and a group of users of a low-service level are allocated placebo keys providing no security, thereby to obviate a need to reconfigure other user's keys upon their invalidation (0090; 0138; 0139).

As per claim 9:

Sudia discloses a method, wherein the service is a dynamic service and its value is ephemeral and based upon its contemporaneous nature (0138; 0139).

As per claim 13:

Lotspiech discloses a computing entity adapted to manage distribution of security keys keys generated from an ancestral hierarchy and used to provide selective access to provision of a service, wherein invalidation of a key necessitates reconfiguration of each other key within the

hierarchy to the extent another key and an invalidated key share common ancestry, the entity being adapted to:

define at least two groups of users of the service to whom keys have been issued (column 3: lines 5-21; column 4: lines 37-60; column 6: lines 20-37);

issue keys to users from domains within the hierarchy upon the basis of their grouping (column 3: lines 11-20, lines 53-64; figure 4:36, 38; Column 7: lines 55-65).

Lotspiech does not explicitly disclose allocate within the hierarchy a distinct domain for each group of users. Sudia, in analogous art, however, teaches allocate within the hierarchy a distinct domain for each group of users (0046-0050). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Lotspiech to include allocate within the hierarchy a distinct domain for each group of users. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to provide a system for securely using digital signatures in a commercial cryptographic system that allows industry-wide security policy and authorization information to be encoded into the signatures and certificates by employing attribute certificates to enforce policy and authorization requirements as suggested by Sudia in (0024).

9. Claims 10-12 and 14 rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia et al. (hereinafter referred to as Sudia, US Pub No.: 2002/0029337) in view of Lotspiech et al. (hereinafter referred to as Lotspiech, US Pat. No.: 7,039,803).

As per claim 10:

Sudia discloses a method of managing security key distribution to a plurality of users of a service comprising the steps of:

defining levels of service provision (0014; 015; 0075); and

allocating keys to users which are indicative to a service provider of the level of service to which they are entitled (Column 4: lines 37-50; column 10: lines 3-22).

Sudia does not explicitly disclose for at least one level of service provision allocating placebo keys which do not provide security for the provision of the services. Lotspiech, in analogous art, however, teaches for at least one level of service provision allocating placebo keys which do not provide security for the provision of the services (column 7: lines 15-25: short-lived key). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Sudia to include for at least one level of service provision allocating placebo keys which do not provide security for the provision of the services. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to provide a grouping of users into (possibly overlapping) subsets of users, each subset having a unique, preferably long-lived subset key, and assigning each user respective private information as suggested by Sudia in (column 3: lines 10-20).

As per claim 11:

Sudia discloses a method, wherein the placebo keys operate in such a manner that a user is not able to perceive a difference between a functioning security key and a placebo key (Column 4: lines 36-52: short and long lived key).

As per claim 12:

Sudia discloses a method, wherein the service is dynamic and its value is ephemeral and based upon its contemporaneous nature (Column 4: lines 36-52: short and long lived key).

As per claim 14;

Sudia discloses a method of computing entity adapted to manage security key distribution to a plurality of users of a service by:

defining levels of service provision (0014; 015; 0075);

allocating keys to users which are indicative to a service provider of the level of service to which they are entitled (Column 4: lines 37-50; column 10: lines 3-22).

Sudia does not explicitly disclose for at least one level of service provision allocating placebo keys which do not provide security for the provision of the services. Lotspiech, in analogous art, however, teaches for at least one level of service provision allocating placebo keys which do not provide security for the provision of the services (column 7: lines 15-25: short-lived key). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Sudia to include for at least one level of service provision allocating placebo keys which do not provide security for

the provision of the services. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to provide a grouping of users into (possibly overlapping) subsets of users, each subset having a unique, preferably long-lived subset key, and assigning each user respective private information as suggested by Sudia in (column 3: lines 10-20).

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See the notice of reference cited in form PTO-892 for additional prior art.

Contact Information

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784 and fax number is (571) 273-3784. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

T-G

Techane Gergiso

Patent Examiner

Art Unit 2137

March 28, 2007

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER